(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 October 2002 (31.10.2002)

PCT

(10) International Publication Number
WO 02/086732 A1

(51) International Patent Classification[7]: G06F 12/16

(21) International Application Number: PCT/KR02/00712

(22) International Filing Date: 18 April 2002 (18.04.2002)

(25) Filing Language: Korean

(26) Publication Language: English

(30) Priority Data:
2001/22334 25 April 2001 (25.04.2001) KR

(71) Applicant *(for all designated States except US)*: **SUNGJIN C & C, LTD.** [KR/KR]; 1543-6 Core Building Secho-dong, Seocho-ku, Seoul 137-073 (KR).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **LIM, In-Keon** [KR/KR]; 100-304 Banpo APT Banpo Bon-dong, Seocho-ku, Seoul 137-049 (KR). **JEONG, In-Hyo** [KR/KR]; 103-1101 Dongbu APT, 691, Suji-ub, Pungdukchon-li, Yong-In City 449-846 (KR).

(74) Agent: **WON, Tae-Young**; Samhee Patent & Law Office, Suite 1905, Sung-Ji Heights III Building, 642-6 Yeoksam-dong, Gangnam-ku, Seoul 135-717 (KR).

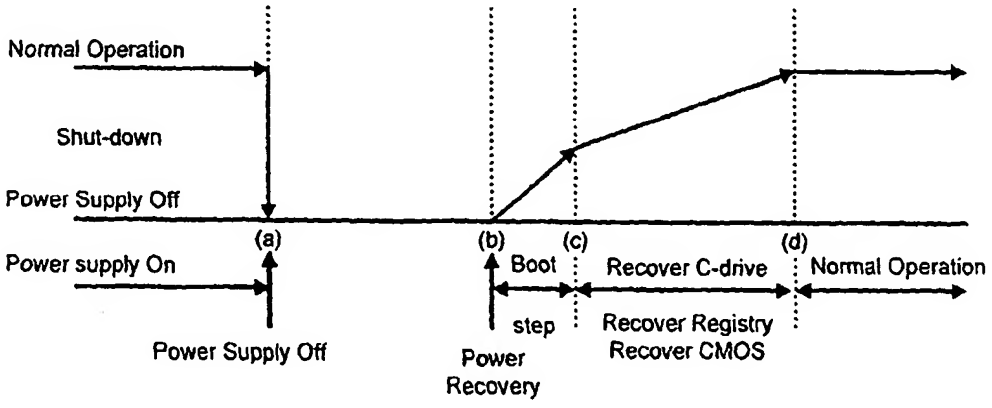
(81) Designated States *(national)*: AU, CA, CN, JP, RU, US.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: APPARATUS AND METHOD FOR PROTECTING FAILURE OF COMPUTER OPERATING SYSTEM



(57) Abstract: The present invention discloses a novel method and apparatus for ensuring that the computer system does not fail to boot under any circumstances. The computer system in accordance with the invention never fails to boot due to the damage at the hard disk containing the operating system even under the abrupt interruption of power supply. The computer system in accordance with the invention comprises an invisible storage region that backs up the operating system. BIOS set-ups, and registry files for booting.

WO 02/086732 A1

TITLE OF INVENTION

APPARATUS AND METHOD FOR PROTECTING FAILURE OF COMPUTER OPERATING SYSTEM

FIELD OF THE INVENTION

The present invention relates to an apparatus and method for protecting the computer hard disk containing the operating system from being damaged due to the abrupt interruption of electric supply which makes it impossible for the computer to reboot when the electricity resumes.

More particularly, the present invention relates to a computer system, such as a control computer for a digital video recorder(DVR), which has a feature that it never fails to reboot the operational system by itself when the electricity resumes after the electric interruption.

The security computer system, which monitors the visual data transmitted from security cameras, is requested to succeed in completing the rebooting process and restore to the previous condition prior to the interruption by power failure without any external help from

the operator.

The present also provides an apparatus and method for protecting the computer operating system (OS) at an instant of power failure.

In case when the electricity feeding the computer system is abruptly interrupted, and more particularly when the power failure occurs during the recording period of data at the hard disk, the file allocation table (FAT) that indexes the stored files is frequently damaged.

As a consequence of the damage of the FAX, it becomes impossible to reboot the system even when the electricity resumes.

As an approach to prevent the hard disk from being damaged due to the abrupt interruption of power supply, an apparatus called UPS (uninterruptible power supply) is widely used. The detailed art for the UPS is disclosed in the gazette of Korean Patent laid-open No. 95-10276.

The technology of the UPS is based upon the preparation of the battery that supplies the electricity for a few minutes in case of the power failure and lets the system undergo the normal shutdown process for the protection of the operating system.

Fig.1 illustrates the process of

rebooting the computer system having a built-in UPS in accordance with a prior art. Referring to FIG.1, when electric power is abruptly cut off at a point (a), the battery prepared in the UPS starts to operate for a selected period of time, from (a) to (b), and then supplies the computer system with the electricity.

After a pre-defined period of time (for instance, one minute), the automatic shutdown process is taken at step (b) in a safe manner.

Consequently, the shutdown process is terminated without damaging the hard disk at the point (c).

Now when the electricity resumes at step (d), the computer starts to reboot automatically and enter the normal operating mode at step (e) without the external operator's assistance.

Since the security system is expected to operate for twenty four hours under any circumstances, the UPS is employed in an effort to avoid the damage of the computer system even in the case of the power failure.

Despite the installation of the UPS at the security system, the security system is sometimes irrevocably damaged during the power failure due to the malfunctioning of the battery.

Further to the frequent malfunctioning

of the battery, it is necessary for the system manager to check the lifetime of the battery and replace it from time to time in order to make sure that the security system works under any circumstances.

Furthermore, it is practically impossible for the system manager to cover the maintenance of all the UPS batteries distributed at so many places.

In addition, since the security camera is shutoff even in the case of the system with the UPS, the UPS system does not make any difference in the aspect of the continuity of the video recording.

SUMMARY OF THE INVENTION

Accordingly, it is an object of the present invention to provide an apparatus and method of preventing the irrevocable damage of the computer hard disk in case of an abrupt power failure and resolving the consequent incapability of rebooting process.

It is further an object of the present invention to provide an apparatus and method for protecting the computer operating system from being damaged by an abrupt interruption of power

supply so that the computer reliably operates twenty four hours a day even without the UPS.

It is another object of the present invention to provide an apparatus and method for restoring the constitution of the operating system of the security computer, the registry, and CMOS set-up in a software manner when the electricity resumes after an abrupt interruption of power supply.

BRIEF DESCRIPTION OF THE DRAWINGS

Further feature of the present invention will become apparent from a description of a method and apparatus for protecting failure of computer operating system taken in conjunction with the accompanying drawings of the preferred embodiment of the invention, which, however, should not be taken to be limitative to the invention, but are for explanation and understanding only.

In the drawing:

FIG.1 is a schematic diagram illustrating the rebooting process of a computer system having a built-in UPS in accordance with the prior art.

FIG.2 is a schematic diagram

illustrating the rebooting process that restores the previous condition software-wise without UPS in accordance with the present invention.

FIG.3 is a schematic diagram illustrating the constitution of the hard disk for back-ups, partitioned in accordance with the present invention.

FIG.4 is a schematic diagram illustrating the process of rebooting the computer system upon the recovery of the electricity in accordance with the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT OF THE INVENTION

The present invention will be explained in detail with reference to the accompanying drawings.

FIG.2 is a schematic diagram illustrating the process of restoring the system in accordance with the present invention. Referring to FIG.2, at step (C), i.e. the interruption of the power supply caused either by a sudden power failure or by other reasons, the protection system in accordance with the invention let the computer system shut down

whatever damage is done and let the computer reboot successfully with the operating system safely stored.

As a consequence, the present invention resolves the problems of the prior art such as the malfunction or the lifespan of the UPS battery.

Namely, referring to FIG.2, if the power supply is interrupted at step (a), system is shut down as it does without any special protection scheme like auto-shutdown method.

Consequently, it may happen that the hard disk can be damaged if the power failure occurs when the FAT is being written. However, the damage at the hard disk does not affect the successful rebooting process of the computer system when the electricity resumes because the damage is repaired software wise according to the present invention.

In case when the power supply is restored at step (b), as illustrated at FIG.2, computer system is ready to start re-booting while the BIOS program normally initiates the operation.

At this time, computer system checks the value of a first flag stored in the pre-defined location in the C-drive, and determines if the

computer system has been terminated either normally or abnormally during the process of the most recent system termination. That is, a first flag indicates how the system has been terminated, i.e. either in a normal procedure of shutdown or in an abrupt termination due to power failure. Preferably, a first flag can be stored at a pre-defined location at drive C.

If the first flag indicates the abnormal termination during the most recent shutdown process, the files for the operating system stored at an invisible storage region are copied to the disk drive C for restoration.

Here, the invisible storage region means a reserved region of a disk drive that is not accessible during a normal operation of the computer.

In other words, since the computer user has neither the recognition nor the access to the invisible storage region for writing and reading the data under the normal operation unlike drives C, D, and E, the invisible storage region is a safe place even at an abrupt interruption due to power failure.

In the claims of the present invention, the invisible storage region according to the present invention is cited as a first storage

region, while the accessing drives C and D are called as a second storage region and the drive for storing data files is called as a third storage region.

During the restoring process, the application files, the registry files, and the BIOS CMOS set-ups are restored as well as the system operation files.

When the system back-ups from the invisibles storage region has been finished, the status of a first flag at drive C is set, followed by a re-booting process under the restored operating system at drive C.

More preferably, once the operating system for the re-booting process has been restored in accordance with the invention, the damaged data at data disk D, for instance, by employing the function of ScanDisk of the operating system.

Moreover, once the process of ScanDisk has been completed, the registry can be normally recovered from the back-ups. Thereafter, a window is popped up and the status of a first flag is set.

In the detailed description of the present invention, an embodiment in accordance with the present invention is introduced such

that disk drive C is designated for storing the system files, while drives D and E are designated for storing data files.

However, the method of partitioning the series of hard disk need not be limited to the above-mentioned embodiment and various embodiments can be employed to implement the scope of the invention.

FIG.3 is a schematic diagram illustrating the constitution of the partitioned hard disk as a preferred embodiment in accordance with the present invention.

Referring to FIG.3, a zero-th hard disk is partitioned as drive C (10), drive D (20), the invisible storage region (30), while a first hard disk is assigned as drive E.

Although a zero-th physical hard disk is partitioned as drive C (10), which corresponds to a first drive in the appended Claims, and an invisible drive (30) for back-ups in the aforementioned embodiment in accordance with the invention, those skilled in the art should understand that a variety of embodiments are acceptable.

As a preferred embodiment in accordance with the invention, the system operating files as well as the windows program are stored at

drive C (10), while the data files are stored at drive D (20) and E (40).

In FIG.3, are also shown FAT (file allocation table; 12) and link files. As aforementioned, the prior art has suffered from the problem of being unable to re-boot the system since the system cannot read the link-file information at drive C due to the damaged FAT II at the abrupt power failure.

In an effort to resolve the above-mentioned problem of the prior art, the present invention has a feature in a sense that an invisible storage region 30 is separately reserved for the back-ups. The invisible storage region 30 implies a storage space which is recognized for the access neither by a user nor by the operating system itself. Since the invisible storage region 30 is not accessed during the normal operation of the computer, the system data stored in the invisible storage region cannot be damaged even at an abrupt interruption of electricity.

The present invention has a feature that the system operating files as well as the windows registry files, BIOS CMOS set-up files stored at drive C are backed up at the invisible storage region for restoration during the

rebooting process when the power resumes.

As a preferred embodiment in accordance with the invention, the operating system (OS) files and the application files can be backed up at the invisible storage region as a factory default when the computer system is initially assembled by the manufacturer.

More preferably, the BIOS CMOS set-up files as well as the OS files can be backed up at the invisible storage region 30 at the stage of the initial factory back-up.

In the meanwhile, it is usually for the user to change all sorts of computer set-ups while the computer is used. For instance, the data compression rate or the control commands are usually set up by the user rather than using the factory default for the security-purpose digital video recorders (DVRs).

The set-up files like the aforementioned data compression rates are called registry files, the updated files of which are usually saved at C:\WINDOWS\SYSTEM.DAT or C:\WINDOWS\USER.DAT under windows system.

Since the back-up files saved in the invisible storage region at drive C is the factory default, the registry files updated by the user can not be completely restored even if

the system is restored only by the back-up files stored at the invisible storage region.

As a consequence, the registry files should be updated once again by the user even if the system is restored by the back-up OS stored at the invisible region.

Moreover, it is not desirable to let the security computer system resume to the set-up conditions of the factory default when the electricity resumes from the power failure. In other words, the security-purpose computer system controlling the digital video recorder (DVR) should return exactly to the most recent status at an instant of power failure in order to guarantee the continuous operation.

Therefore, the present invention resolves the afore-mentioned problem by updating the back-up files like registry files at the invisible storage region 30 from time to time.

Preferably, every time when the set-ups of the registry are changed, the back-up files stored at the invisible region 30 should be updated.

More preferably, the frequency of the update of the registry files at the invisible storage region 30 can be adjusted in such a way that the updating process does not burden the

workload of the central processing unit (CPU).

As a preferred embodiment in accordance with the invention, the size of the invisible storage region can be chosen as 810 MB if the capacity of the drive C is 800 MB and the file size of the registry is 5 MB.

In the meanwhile, once the system restoration has been completed, the possibly damaged data files at drive D or E can be repaired through the ScanDisk command of the windows program.

More, in case the upgraded versions of the system operating files or of the application files (for instance, the control program for monitoring the security-purpose digital video recorder) have been installed additionally, it is possible to prevent the system to return to the factory default state during the restoration step by the method set forth below.

Since the system files that are backed up at invisible storage region are the ones that were initially stored at a step of factory shipment, it is necessary to upgrade those backed-up system files at the invisible storage region if the system files have been upgraded.

Preferably, the system operating files backed up at the invisible storage region 30 can

be upgraded by performing an additional step of updating the back-up files every time when the operating system is upgraded. More preferably, once the upgraded version of system files has been installed, backup files can be upgraded if the user consents to upgrade.

Moreover, in case that new device driver files including printer driver files have been installed, the back-up files at the invisible storage region can also be updated.

FIG.4 is a flowchart illustrating the process of re-booting the computer system in accordance with the present invention.

Referring to FIG.4, once the electricity resumes (step S100), the computer system starts to reboot, and executes the BIOS program (step S110).

Thereafter, the computer system checks the value of a first flag, which indicates whether the system has been terminated in a normal shutdown procedure or not (step S120).

Preferably, the value of a first flag stored at a pre-defined location is set to in case the system terminated abnormally during the most recent system termination, while it is reset to zero in case of normal shutdown.

If the first flag implies the normal

shutdown at the instant of previous termination, the system is re-booted under the normal procedure.

Preferably, the system is implemented in such a way that a second flag, which indicates whether the application program or the device files have been upgraded or not, can be referred to.

In other words, the upgraded programs and/or the information about the recently installed printer driver are backed up at the invisible storage region, and thereby it is possible to prevent the system from returning to the state of factory default upon restoration.

A second flag can be used for carrying out the above-mentioned process. Referring to FIG.4, the system performs the restoring process from the back-up drive C (10) at the invisible storage region in case when the second flag is set (step S121).

In the meanwhile, the system follows the normal booting procedure and executes the windows operating program (step S130) if the second flag is not set at step S121.

As a consequence, the windows program is executed while a first flag is set in order to make sure to provide the mode of the next time

shutdown process (step S140). Thereafter, the application program is executed (step S150).

As a preferred embodiment in accordance with the present invention, the security operating system can be executed.

More preferably, the change in computer set-ups can update the windows registry for a pre-defined period of time (for instance, every 30 seconds) after the setting window is closed.

Preferably, the upgrade of the application program or the printer driver file can make the system raise an inquiry about the user's consent whether the back-up is updated or not (step S155).

At step S155, if the user consent with updating the backup, the process for the system shut-down is initiated, followed by the first and setting of a first and a second flags (step S156).

Further, if the user does not agree with updating the system back-up, the computer system operating a user's application program is shutdown, followed by the process of setting the first flag in order to discriminate whether the system terminates normally at a time of the next booting (step S160).

Thereafter, a first flag is reset with

the ending process of the windows program (step S170).

In the meanwhile, in case when flag has set at step S120, the system recognizes that the system has been terminated abnormally and then restores the disk drive C by copying the backup files, which have been saved at the invisible storage region of the hart disk (30) (step S230).

Thereafter, Once the restoration of the system has been completed, a first flag and a second flag are all reset, followed by a re-booting process (step S240).

Simultaneously, damaged data files at drives D or E can be repaired by the ScanDisk command (step S250).

Once the data files are restored (step S250), the registry is recovered (step S260) and thereafter a first flag at drive C is set (step S270) with the execution of windows program.

The process steps S150, S160, and S170 are followed thereafter.

Moreover, in case of manually upgrading the application program or the driver files, the back-up files can also be updated by selecting system backup menu after the program installation.

In this case, since a second flag is set

at step S121, the system copies the whole files from the invisible storage region of the hard disk for re-booting (step S122).

Thereafter, a first flag as well as a second flag is reset, followed by a re-booting process (step S123). Moreover, a ScanDisk process (step S124) is followed by the execution of the windows program. Finally, a first flag is set (step S125) and the application program is executed (step S150).

Although the invention has been illustrated and described with respect to exemplary embodiments thereof, it should be understood by those skilled in the art that various other changes, omissions and additions may be made therein and thereto, without departing from the spirit and scope of the present invention.

Therefore, the present invention should not be understood as limited to the specific embodiment set forth above but to include all possible embodiments which can be embodies within a scope encompassed and equivalents thereof with respect to the feature set forth in the appended claims.

WHAT IS CLAIMED IS:

1. A method for booting the computer system, the hard disk of which is partitioned into a multiple of storage regions wherein a first storage region is an invisible region that the user is not allowed to have an access to and a second storage region storing the operating system, the first storage region being the back-up of the second storage region, comprising steps of:

(a) checking the value of a first flag, which indicates the condition of the last termination, i.e. the normal shutdown or the abrupt interruption due to power failure, when the electricity resumes and the BIOS program starts to be executed;

(b) restoring said second storage region by copying the files backed up at said first storage region in case when said first flag is set (abnormal termination), and then resetting said first flag and said second flag that manually indicates whether the contents stored at said second storage region is at said first storage region, followed by a re-booting process;

(c) checking said second flag in case the value of said first flag is reset (normal

termination) at a step of (a)

(d) performing the back up of the contents stored at said second storage region onto said first storage region in case said second flag is set (request for manual back-up) at a step of (c), followed by a re-booting process with said first flag and said second flag reset;

(e) performing normal booting process and windows program and setting said first flag incase said second flag is reset (not requesting manual backup) at a step of (c); and

(f) executing the application program.

2. The method as set for the in Claim 1 wherein said step of (b) is followed by steps of:

Performing ScanDisk in order to restore a third storage region from damage, which stores the data files for said computer system; and

Restoring the registry of said computer system, and operating the windows OS, followed by a setting process of said first flag.

3 The method as set forth in Claim 1 wherein said step of (d) further comprises steps of:

Performing ScanDisk in order to restore a third storage region from damage, which stores

the data files for said computer system; and

operating the windows OS, followed by the setting process of said first flag.

4. The method as set forth in Claim 1 further, following said step of (f), comprises steps of:

(g) backing up the contents of said second storage region onto said first storage region upon the order of the computer user in case when the computer operating system has been either upgraded or additionally installed;

(h) performing the system shut-down first flag and setting said first flag and said second flag if the manual restoration has been selected at a step of (g);

(i) performing the system shut-down procedure and setting said first flag if the manual restoration has not been selected at a step of (g); and

(j) closing the windows program, followed by resetting said first flag.

5. The method as set forth in Claim 1 wherein said first storage region stores back-ups of:

BIOS CMOS setup files or factory default files stored at said second storage region;

registry files for system operation

updated by the computer user while using the computer;

device driver files installed additionally or upgraded files installed at said second storage region while using the computer; and

software program for performing the backup procedure.

6. A computer system, the hard disk of which is partitioned into a multiple of storage regions wherein a first storage region is an invisible region that the user is not allowed to have an access to and a second storage region storing the operating system, comprising:

a first flag indicating whether the computer system has been shutdown normally or abnormally at the most recent instant of termination; and

a second flag indicating that the updated contents such as the upgraded program files or the additionally installed device drive files at said second storage region should be backed up at said first storage region, wherein once the BIOS program starts to be executed at the initiation step of booting, the computer system is rebooted by the backed-up OS files stored at

said first storage region when said first flag is set (abnormal termination); whilst the backed-up files are stored at said second storage region is copied to said first storage region when said first flag is reset (normal termination) and said second flag is also set (manual back-up); whilst the normal booting process is performed by the system operating files stored at said second storage region when said first flag and said second flag are all reset.

7. The computer system as set forth in Claim 6 wherein said first storage region stores the backups of system operating files, BIOS CMOS files, and system operating registry files, while the control program for backup process is stored at said first storage region that is invisible to the computer user.

8 The computer system as set forth in Claim 6 wherein said hard disk further includes a third storage region for storing data files, and if said first flag indicates the abnormal shutdown at the instant of the last termination, said third storage region is repaired by the windows command ScanDisk and the registry is restored.

9 The computer system as set forth in Claim 6 wherein if the system operating files stored at said second storage region are upgraded during the use of the computer, the upgraded system operating files are backed up at said first storage region, and thereby the system is booted with the upgraded system operating files.

10 The computer system as set forth in Claim 6 wherein if a device driver file including a printer driver file is additionally installed during the use of the computer system, the driver file stored at said second storage region is backed up at said invisible first storage region, and the additionally installed driver file can be recognized during the re-booting step after the abnormal termination.

11. The computer system as set forth in Claim 6 wherein said system operating registry files comprise system data file (SYSTEM.DAT) and the user's information file (USER.DAT) under windows operating system.

12. A method for booting the computer system, the hard disk of which is partitioned into a multiple of storage regions wherein a first

storage region is an invisible region that the user is not allowed to have an access to and a second storage region storing the operating system, BIOS COMS set-ups, and registry files that are updated during the use of the computer system, the first storage region being the back-up of the second storage region, comprising steps of:

(a) supplying electricity to said computer;

(b) executing said BIOS program as the booting process is initiated;

(C) checking the state of a first flag which indicates the status of the last system shutdown, i.e. normal termination or abnormal termination such as due to abrupt power failure;

(d) restoring said second storage region to the previous state prior to the last termination by reading out files from said invisible first storage region and writing them onto said second storage region if said first is set at the step of (c);

(e) resetting said first flag and a second flag that indicates the manual backup process, followed by the rebooting process;

(f) executing windows ScanDisk command at a third storage region storing data files;

(g) restoring registry that has been backed up at said invisible storage region; and

(h) executing windows operating program, followed by setting said first flag.

13. (a) supplying electricity to said computer;

(b) executing said BIOS program as the booting process is initiated;

(C) checking the state of a first flag which indicates the status of the last system shutdown, i.e. normal termination or abnormal termination such as due to abrupt power failure;

(d) checking the state of a second flag which indicates the order to backup the contents of said second storage region onto said first storage region if said first flag is reset.

(e) backing up the contents at said second storage region onto said first storage region if said second flag is set (manual backup);

(f) resetting said first flag and said second flag, followed by the re-booting process;

(g) restoring registry that has been backed up at said invisible storage region; and

(h) executing windows operating program, followed by setting said first flag.

14. (a) supplying electricity to said computer;

(b) executing said BIOS program as the booting process is initiated;

(C) checking the state of a first flag which indicates the status of the last system shutdown, i.e. normal termination or abnormal termination such as due to abrupt power failure;

(d) checking the state of a second flag which indicates the order to backup the contents of said second storage region onto said first storage region if said first flag is reset.

(e) executing the windows program under the normal booting procedure if said second flag is reset; and

(f) setting said first flag.

15. The method for booting the computer system as set forth in Claims 12, 13 or 14 wherein said method further comprises steps of:

executing the application program stored at said second storage region;

making an order to back up the data of said second storage region onto said first storage region;

shutting the computer system down and setting said first flag and said second flag;

and

closing said windows program and resetting said first flag.

16. The method for booting the computer system as set forth in Claims 12, 13 or 14, wherein said method further comprises steps of:

executing the application program stored at said second storage region;

making an order not to back up the data of said second storage region onto said first storage region;

shutting said computer system down and setting said first flag and second flag; and

closing said windows program and resetting said first flag.

FIG. 1

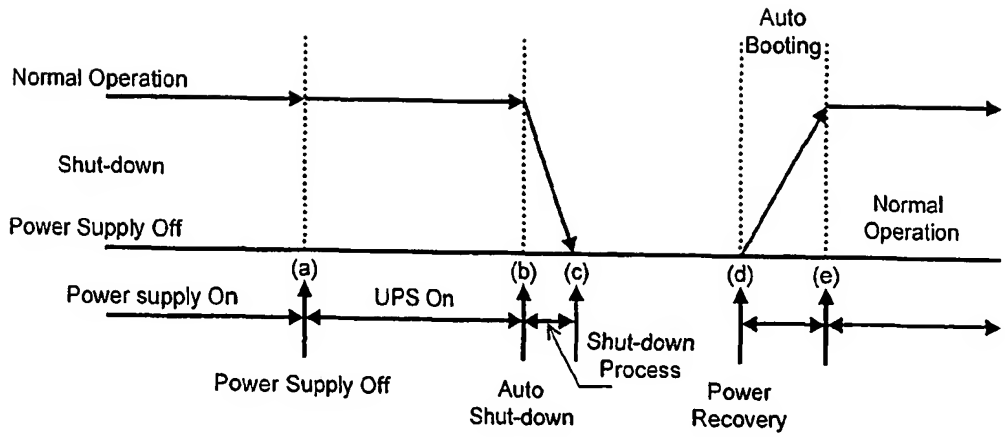

Auto
Booting
Normal Operation
Shut-down
Power Supply Off
Normal
Operation
(a)
(b)
(c)
(d)
(e)
Power supply On
UPS On
Shut-down
Process
Power Supply Off
Auto
Shut-down
Power
Recovery

FIG. 2

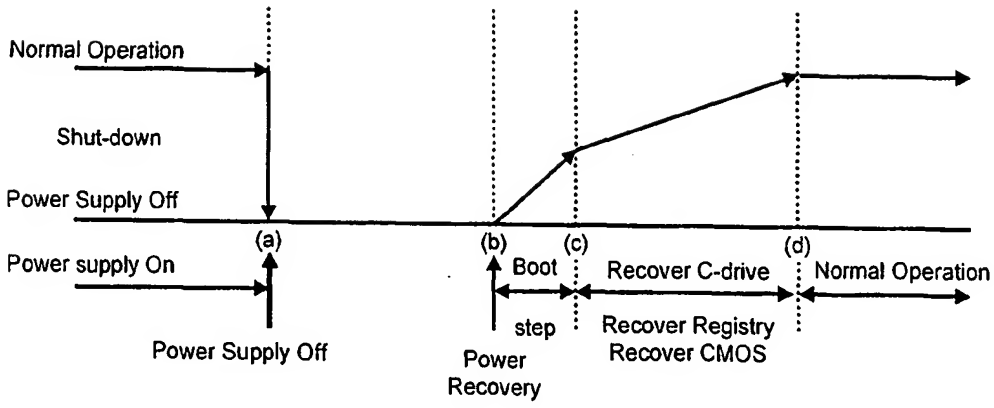

Normal Operation
Shut-down
Power Supply Off
Power supply On
Power Supply Off
(a)
(b)
(c)
(d)
Boot
Recover C-drive
Normal Operation
step
Power Recovery
Recover Registry
Recover CMOS

FIG. 3

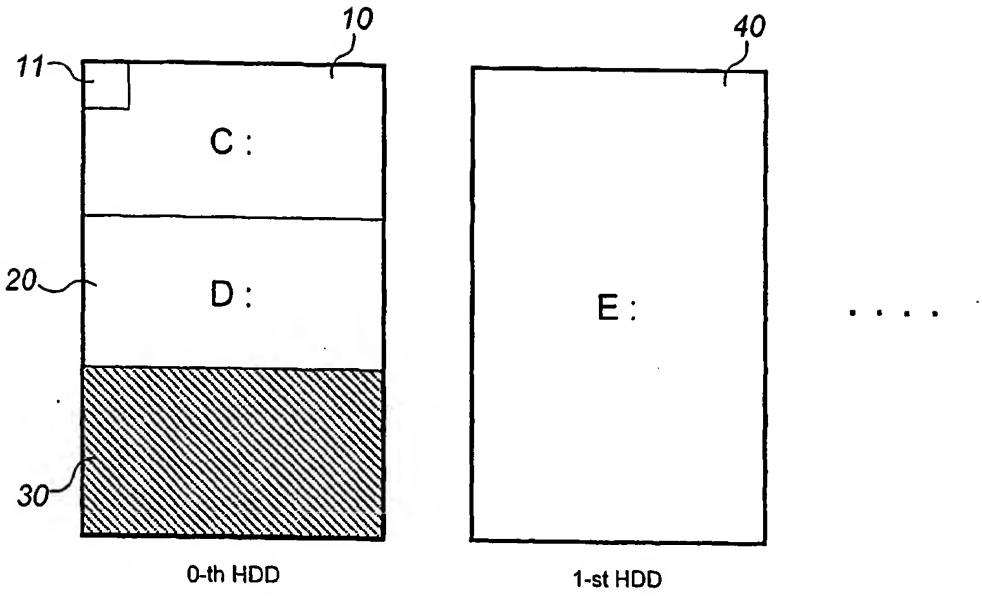
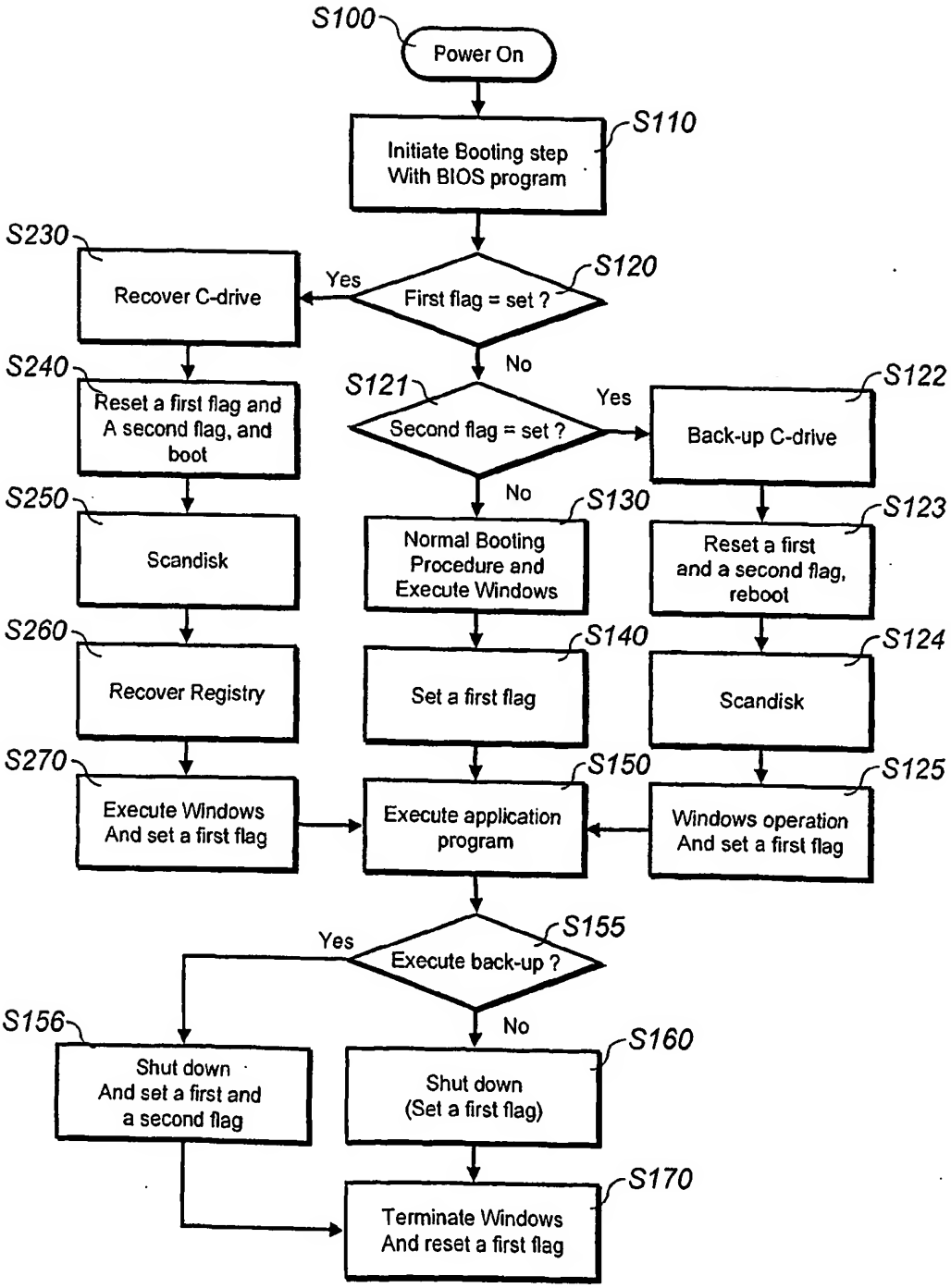


FIG. 4


S100
Power On
Initiate Booting step With BIOS program
S110
First flag = set ?
S120
Yes
No
Recover C-drive
S230
Second flag = set ?
S121
Yes
No
Back-up C-drive
S122
Reset a first flag and A second flag, and boot
S240
Scandisk
S250
Normal Booting Procedure and Execute Windows
S130
Reset a first and a second flag, reboot
S123
Recover Registry
S260
Set a first flag
S140
Scandisk
S124
Execute Windows And set a first flag
S270
Execute application program
S150
Windows operation And set a first flag
S125
Execute back-up ?
S155
Yes
No
Shut down And set a first and a second flag
S156
Shut down (Set a first flag)
S160
Terminate Windows And reset a first flag
S170